Policy	International Travel Security Policy
Impact	Data, Technology, and IT Resources
Responsible Office	Academic, Student Affairs, IT Services
Created	December 9, 2022
Reviewed	June 23, 2025
Approved by	VP for Finance and Administration
Version	25.1

INTERNATIONAL TRAVEL SECURITY POLICY

PURPOSE

Information assets and IT resources that contain, distribute, and store data are vital to the systems that support Shepherd University's ongoing mission of discovery, learning, and engagement. The purpose of this policy is to define minimum requirements for the acceptable use of university-owned and personally owned devices being utilized and/or accessing Shepherd University networks and/or IT resources remotely, while traveling abroad.

POLICY

To ensure all international travel is properly authorized: (1) all faculty and staff users will need to obtain and supply written permission from the appropriate Executive Team member supporting proposed travel and accessibility to use Shepherd University information assets, IT resources, or access to Shepherd University networks while abroad; (2) all students and individuals participating in a university sponsored education experience and/or organized travel will need to adhere to this policy for guidance on usage of their personal devices. Particular care should be taken for proposed travel to countries, specific regions, or cities which the U.S. Department of State has designated as medium or high risk.

No access to Shepherd University networks or IT resources will be permitted/granted if travel is to any embargoed country, as designated by the U.S. Department of State.

UNIVERSITY-OWNED DEVICES

- To ensure proper security, users are required to visit IT Services at least 2 weeks prior to international departure, in order to review security standards and best use including, but not limited to:
    - All devices must be running the latest operating system.
    - All devices must have the latest version of anti-virus.

    - All devices are required to be configured/locked for re-authentication, if left unattended for more than 5 minutes.
    - All devices are required to adhere to whole disk encryption, regardless of operating system.
    - All university data and/or programs/applications not required for the purpose of the international travel must be removed. All remaining applications must be up-to-date with the latest security patches.
- Bluetooth and Wi-Fi must be disabled, unless actively engaged with these functions.
- University-owned equipment must remain with the traveler/user at all times. Do not assume a hotel safe is a secure place to store a university-owned device.
- University-owned equipment is not permitted to be taken to any embargoed country.
- All USB and/or CDs/DVDs must be encrypted.
- Only plug-in accessories owned by user and brought for international use is permitted. Use of unknown USB devices is prohibited, as it can contain malware.
- Public USB charging stations at international airports, hotels, and others should be avoided.
- If any university-owned device is lost or stolen while abroad, the Information Privacy Officer must be contacted immediately and informed of the Security Incident.
- Upon return to the U.S., all university-owned devices used for any international travel must be immediately delivered to Shepherd University IT Services so that the device can be erased and reimaged, either from a backup or through a new installation, prior to connecting to the campus network.
- Travelers are not permitted to spend more than 12 months outside of the U.S. with either a university-owned device and/or maintain access to Shepherd University IT networks or IT resources.

ACCESS to UNIVERSITY NETWORKS or SYSTEMS

Secure, access to university networks or systems while abroad requires strong encryption at all times.

- Access to Sensitive data must not be accessed at any time when traveling abroad.
- Connect utilizing a virtual private network (VPN), when possible (contact IT Services).
- If connecting via a public Wi-Fi and a VPN is unavailable, Citrix must be utilized to gain the appropriate access (contact IT Services). *Please note*: may require prior approval to utilize.
- Public workstations in cybercafés, libraries, hotels, or foreign institutions must not be used to access Shepherd University networks, systems, or IT resources.
- Passwords and university credentials used abroad, must be changed immediately upon return to the U.S. (contact IT Services).

PERSONALLY-OWNED DEVICE SECURITY

If a personally-owned device, including a smartphone, is taken abroad with the intention of accessing Shepherd University networks or IT resources, it must adhere to the following minimal requirements:

- Must have a passcode
- Must be configured to lock and require re-authentication if left unattended for more than 5 minutes.

- Must be able to provide native encryptions, if setting a passcode did not automatically encrypt your device.
- Ensure all operating systems are up-to-date.
- Install anti-virus, and ensure it is up-to-date.
- Refrain from downloading any new applications while outside of the U.S.
- Ensure a proper back up for each device has been created.
- Enable "find my device" to be able to wipe contents remotely, if necessary.

PRIVACY, OPERATIONS, and MONITORING

Shepherd University seeks to maintain its IT environment and manage all information assets including data, computing devices, systems technology, telephony, and IT resources in a manner that respects individual privacy and promotes user trust. However, the use of Shepherd University IT resources is not completely private, and users should have no expectation of privacy in connection with the use of any information asset or IT resource.

Shepherd University has the legal right to access, preserve, and review all information stored on or transmitted through any information asset or IT resource, including the inspection of e-mail messages, logging of activities, monitoring usage patterns, and data audits/integrity checks. IT Services may, with or without notice to users, take any other action it deems necessary to preserve, secure, and protect systems, information assets, or IT resources for the betterment of Shepherd University. Without limiting its right to take action, Shepherd University may, it is sole discretion, disclose the results of any general or individual monitoring or access permitted by this policy, including the contents and records of individual communications, to appropriate Shepherd University personnel and/or law enforcement agencies.

SCOPE of AFFECTED PARTIES

This policy applies to all users, such as students, faculty, and staff of Shepherd University, as well as any other persons attempting to access Shepherd University information assets and/or IT resources while traveling abroad.

ROLES & RESPONSIBILITIES

All Shepherd University students, faculty, staff, and other parties with access to Shepherd University information assets and IT resources shall be responsible for:

USERS

- Understand and comply with the guidance provided by this policy, as well as applicable compliance programs and affiliated awareness training with all applicable laws, standards, procedures, and university protocols.
- Physically secure and safeguard university-owned equipment, as well as any personally-owned equipment being utilized to access Shepherd University information assets or IT resources, within the user's possession and control.
- Understand and adhere to the encryption and access guidelines provided by this policy relating to accessing and using data within any Shepherd University system.

- Promptly report any suspected violation of this policy, any security events, and/or incidents involving a suspected compromise of a user's account or IT resource to itworkorder@shepherd.edu.

CIO/CISO - INFORMATION PRIVACY OFFICER

- Oversee and administer this policy.
- Provide direction to all affiliated departments that partake and/or leverage international travel.
- Provide authorization and direction to IT Services staff in accordance with this policy.
- Develop awareness and necessary training materials as it pertains to this policy.

IT SERVICES STAFF

- With appropriate authorization, take directed action in accordance with this policy to preserve, secure, and protect the interests of Shepherd University.
- Ensure all associated procedures are followed and documented accordingly when taking any actions outlined in this policy.

RELATED TOOLS

RELATED POLICIES & GUIDELINES

- BOG#35: Information Technology Security
- Acceptable Use Policy
- Information Security & Privacy Policy
- Data Classification Policy
- Data Notification Policy
- Password Guidelines
- Social Security Number Guidelines
- Work from Home / Remote Access Guidelines